

Looking Out At The Dark
EMA in a Homeland Security Environment
Paper by
Jim Truscott & Robert Kilsby
Truscott Crisis Leaders

With the PM having foreshadowed the possibility of pre-emptive attacks in the war against terror, how much homeland security is enough in the current global security environment. Indeed is there a role for an Emergency Management Agency in homeland security? In light of the terrorism warning for Australia and the government response of vigilance being the key to countering the terrorist threat, many organizations, businesses in particular, are asking what vigilance exactly means, and what precisely they should be doing? This article aims to provide a better understanding of dealing with the civil disaster risks that terrorism poses domestically.

The government has three key strategies for defeating terrorism through the winning of high-grade intelligence, the option to launch pre-emptive attacks, and consequence management. In implementing these strategies, while the Australian Government is primarily concerned about the crisis issues of ensuring business continuity, maintaining national reputation and minimizing financial and legal liability, all government departments must deal with the coalface tasks of saving life, protecting property and minimizing damage to the environment.

There appears to be a need to make the impact probability business more understandable as it can be complex, and the Australian public is often not comfortable with assessments of low-probability events such as terrorism. People will generally assess risk either analytically or emotionally. The emotional response is generally accepting of natural disasters such as fires and floods, but human actions such as suicide terrorism without apparent boundaries, induces escalating individual and communal fears. In addition to formulae to support natural disaster hazard management, there is need for similar formulae to give an answer to outrage risk assessments of potential man-induced civil disasters.

Firstly, is there a role for EMA to support government efforts in winning high-grade, generally secret intelligence to defeat terrorism? Most civil disaster agencies will be familiar with overt assessments of consequence and likelihood of natural hazards, but with security issues one needs to look at threat a little differently. When looking at terrorist threats, authorities need to think in terms of the terrorist's intent and capability. Intent in turn requires an assessment of both the terrorist's desire and expectation, while capability is a combination of the terrorist's resources and knowledge. The combination of capability and intent is expressed as high, medium, low or insignificant as shown in this matrix.

Stated or known	L	M	H	H
General or suspected	L	L/M	M	H
None suspected	I	L	L/M	M
None confirmed	I	I	L	L
Intent/ Capability	Nil	Limited	Significant	Comprehensive

It can be difficult to assess intent and capability when the terrorist functions from underground cells, and he is unpredictable at best; but you can look at your own assets, and this is what a saboteur does when they are analysing a target within a target system. Saboteur terrorists will use something like the 'CARVER' acronym. Local Emergency Management Advisory Committees (LEMACs) and supporting agencies may also find it useful in assessing threats to assets within their responsibility, particularly if they do not have access to classified reporting. When looked at through the eyes of the adversary, the threat can become a little clearer. In determining what is in a particular council or shire, and whether it is a soft target, a CARVER assessment can be used to look at the critical infrastructure from a terrorist viewpoint.

- **C** is criticality or relative importance. What part of your council or shire is most critical? For example a rural terrorist may seek to destroy the spare parts warehouse for the pumping station or the fire station, in addition to the moving parts in the local manufacturing plant. An urban terrorist may seek to destroy a Disaster Recovery Centre in a capital city, in addition to the critical communications nodes.
- **A** is for accessibility or ease of access. Just getting to the target can be confusing at best in the middle of the night in unfamiliar terrain and urban geography; so easy access targets are often preferred. The terrorist may simply turn up in a taxi.
- **R** is recoverability and how easily the asset can be repaired, replaced or brought back on line. This downtime thinking may indicate a further threat to repair and spare parts facilities, as a terrorist will seek maximum outage or maximum bang for buck.
- **V** is for vulnerability and the ease with which people and infrastructure can be put out of action with a hammer or a computer virus from a soft or hard perspective. Martyrs are just as scared as anyone else when it comes to delivering the final blow, even with the motivation of 70 virgins and a place in heaven. All terrorists will look for the easier way. For example, the Bali bombing is alleged to have only costed the terrorist's about \$30,000.
- **E** is for effect. Terrorists will concentrate on targets that will cause the greatest adverse effect on local population, but also on the national and international communities to meet their overall psychological objective. Information infrastructure and utilities are most at threat here as suicide terrorists favour spectacular attacks that have high symbolic value, cause mass casualties, and severe damage to the economy. Terrorists want the effect to be damaging to all and sundry, by seeking to get the entire nation to go into mourning.
- **R** is for recognition and answering the what is it, and the what, where type questions? It is the ability to actually to identify one target from another. The effect of their action will be minimised and even counter-productive to the terrorist planners' objective if the wrong target is hit, but note that not all local terrorists are as smart as Osama bin Ladin, and some attacks may not be logical.

Secondly, is there a role for EMA in any preventative action against terrorism? It would seem that a proactive attitude, to minimise the need for consequence management, is the key to supporting any domestic preventative action. This outcome is all about achieving a high but cost-effective level of readiness, working in where possible with the Federal Government's campaign to improve the public's awareness of terrorist activities.

In influencing community attitudes, LEMACs have to consider what is the difference between a good level of community security and a bad level of community security. In simple terms, bad security eats you, but good security feeds you. The best money is money, which makes you more money, and so community security needs to be viewed as a contributor to profit, and not as a cost centre.

Just as organizations are humanizing safety to overcome cost centre mentality in the drive towards zero-incidents, so too must security be humanised. In the absence of strategic warning, every employee and every citizen must look out into the dark. Every employee and every citizen must actively report through 1800 numbers. There needs to be a system of collecting security-related information at assets and industrial facilities as intelligence collection will be critical to early warning in the absence of specific government-supplied information about indicators of an attack. Furthermore there needs to be a community system or procedure for lost communications to optimise mutual aid in the real community sense of the word.

Finally, is there anything different about EMA's role in managing the consequences of locally targeted suicide terrorism? The key here is to continue to act locally, but all thinking must be focussed by global events. Local planning must be conducted in the context of world happenings. Area studies, which may currently exist for natural hazards, must be expanded in the security sense to incorporate CARVER assessments of critical infrastructure and its relative importance regionally and nationally.

While the government only identifies about six vital national assets, the same thinking can be applied by LEMACs to the lowest appropriate level. Although there is always an element of unpredictability in dealing with terrorists who plan and act beyond normal and rational thought, thinking from the terrorists' side can be a powerful mechanism for civil disaster agencies in their contribution to homeland security.

	Terrorist Thinking	EMA & LEMAC Thinking
Criticality?	Is it a high-value target?	What are my critical infrastructure and networks?
Accessibility?	Is it easy to reach?	How effective are my layered security measures?
Recoverability?	How long will the outage or outage last?	Do I know how quickly utilities can be restored?
Vulnerability?	How easy is it for me to destroy?	Do I know the critical components of my infrastructure, and what are their security barriers?
Effect on the local population?	Will the psychological effect achieve my aim?	What is likely to generate public pressure?

Recognizable?	What does it look like, and where is it?	Can simple recognition be prevented in some harmless way?

TRUSCOTT TRUSCOTT is a niche consultancy focused on preparing executives and managers for the **Crisis Leaders** unthinkable but, unfortunately, the inevitable.

We consult to organisations large and small throughout Australasia and Asia. We have assisted hundreds of clients in government, multi-national, medium, and small organisations. We have wide experience in the resources, energy, and finance sectors.

Jim Truscott, the founding director of TRUSCOTT, spent 25 years as a strategic group manager and leader of operational teams in high-risk international engagements planning and controlling politically sensitive government operations for the successful resolution of regional and international crises. Drawing on that wide experience, he now consults to industry and government on crisis leadership and on risk and emergency management.

Robert Kilsby is skilled in controlling crises from 20 years in the SAS in totally hostile and confusing situations and now on the second battlefield as a crisis leadership practitioner.

Contact TRUSCOTT at jtruscott@crisisleaders.com or visit www.crisisleaders.com